Cisco Security Architecture Assessment Service

An Architectural Approach to Aligning Integrated Security Infrastructure to FISMA Guidelines

An Architectural Approach to Security and FISMA

Gain a comprehensive view of your security infrastructure while remaining aligned with security policy and compliance requirements as defined by the Federal Information Security Management Act (FISMA):

- **Align security goals with organizational objectives:** Identify and prioritize risks and remediation opportunities.
- **Use standards-based methodologies:** Use the Cisco Security Control Framework to gain visibility and control.
- **Reduce regulatory compliance exposure:** Increase the confidentiality, integrity, and availability of your business processes and information.

Introduction

In today's complex and ever-changing threat landscape, gaps in infrastructure security can place data integrity, information confidentiality, and mission-critical applications at risk. Your agency needs integrated security controls that protect your infrastructure in this dynamic risk environment. An effective way to accomplish this is through a systematic, architectural approach that considers the entire IT lifecycle while remaining aligned with security policy and compliance requirements as defined by the Federal Information Security Management Act (FISMA).

A major part of the FISMA program is the active and near-real-time monitoring and management of government networks, infrastructure, and data. Under FISMA, agencies are expected to perform periodic security assessments to maintain a current picture of their vulnerabilities, allowing them to prioritize remediation activities based on available resources and homeland security risk.

To protect critical federal IT infrastructure from security intrusions (physical and cyber), Cisco offers a comprehensive, in-depth infrastructure security assessment program that addresses FISMA and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 requirements.

Cisco security architecture assessments are conducted using the Cisco® Security Control Framework in conjunction with the government security framework. This framework is built from NIST SP 800-53 standards, security architecture principles, and Cisco engineering experience in securing enterprise infrastructures and information assurance.

Focusing on the technology controls that support the foundational security objectives of visibility and control, the Cisco Security Control Framework is used to evaluate the architecture that protects your extended network infrastructure, attached devices, and mission data. This framework is consistent with NIST SP 800-53 guidelines and standards, as well as industry standards, including the International Organization of Standardization (ISO) 27000 series and Information Technology Infrastructure Library (ITIL® v3).

Cisco Security Architecture Assessment Service

The Cisco Security Architecture Assessment Service allows your agency to implement a comprehensive security architecture by identifying gaps in your security infrastructure and providing a prioritized set of actionable steps to remediate them.

The Cisco Security Architecture Assessment Service addresses security issues in both network and physical security disciplines for borderless networks and connected real estate.

The mission of the Cisco Security Architecture Assessment is to:

- Implement risk-based information security programs
- Establish a level of security due diligence for federal agencies and contractors supporting the federal government
- Consistently apply security controls across the federal information technology infrastructure
- Create a more consistent, comparable, and repeatable security control assessment program
- Enable a better understanding of enterprisewide mission risks resulting from the operation of information systems
- Develop a more complete, reliable, and credible set of data points for authorizing officials in order to facilitate more informed security accreditation decisions
- Provide a more secure information system within the federal government, including the critical infrastructure of the United States

Cisco security experts begin by conducting a detailed review of your security goals and requirements. Based on this information, they complete an in-depth analysis of your security infrastructure, including:

- Operational processes
- Operations management tools
- Network topology
- Network devices
- Security devices

Additionally, they provide an evaluation of your overall security architecture for scalability, performance, and manageability.

Working from carefully gathered data about your infrastructure, Cisco engineers are able to identify vulnerabilities and operational risks in your architecture by performing a thorough analysis of its alignment with industry best practices. Engineers then provide prioritized and actionable recommendations to mitigate the identified operational risks, including improvements to topology, protocols, policy, device configurations, and management tools.

Cisco Security Architecture Assessment Service Domains

In order to provide flexibility in matching your unique business, infrastructure, and budget requirements to FISMA, the Cisco Security Architecture Assessment Service and the underlying Cisco Security Control Framework can be customized to focus on various functional domains in your infrastructure. The Cisco Security Architecture Assessment Service includes one required and six optional assessments:

- Internal Security Architecture Assessment (Required)
- Perimeter Security Architecture Assessment
- Wireless Security Architecture Assessment
- Data Center Security Architecture Assessment
- Physical Security Architecture Assessment
- Security Operations Management Assessment
- Cloud Security Assessment

Cisco Internal Security Architecture Assessment (Required)

Sophisticated cross-protocol client-side attacks that are launched internally are potentially more disruptive and costly than external security breaches. This service examines the security architecture in the internal network required to protect against these threats, including WANs and LANs for core, campus, and individual sites. It also covers common security infrastructure controls that apply to access control, identity management, network management, intrusion detection and prevention, security event management, and logging. This assessment is required because it creates a baseline for the other assessments.

Cisco Perimeter Security Architecture Assessment

Connecting your internal network to the Internet, partners, customers, and your mobile workforce is a primary business enabler, but exposes your infrastructure, intellectual property, customer data, and the availability of your core business services to significant threats. This assessment evaluates the security architecture that protects the boundary between the internal network and external networks, including perimeter firewalls, access control devices, guest networks, employee remote access, and e-commerce sites. This type of assessment work is focused on multilevel cybersecurity networks and trusted Internet connection (TIC) sites.

Cisco Wireless Security Architecture Assessment

Interception, rogue access points, weak encryption keys, and denial-of-service attacks can target your wireless LAN (WLAN) infrastructure. While wireless LANs produce significant productivity gains, if not correctly configured they can be one of the easier locations in the infrastructure to exploit. Properly deploying and configuring your WLAN secures your wireless infrastructure to protect your confidential data and increase availability. This assessment addresses the security architecture that protects the wireless and associated infrastructure, including local and guest controllers, access points, and WLAN clients.

Cisco Data Center Security Architecture Assessment

Internal servers and data center hosts contain business-critical information resources that are generally accessed by trusted users, but internal security is still a serious concern. Properly securing your data center protects it from internal attacks and provides an additional layer of protection in case an external attacker gains entry to your infrastructure. This assessment evaluates the primary data center technologies and components, including the storage network, server farm, services aggregation, core, distribution, access control, and host virtualization so you can fully utilize your data center equipment securely.

Cisco Physical Security Architecture Assessment

Controlling physical access to your facility is a critical component in the overall security of your infrastructure and confidential information. If intruders gain access to your infrastructure, they are in a position to install network back doors, keystroke loggers, software to call home, and rogue access points or compromise other deployed security measures. This assessment covers the controls related to the perimeter and internals of the building or campus, monitoring devices, environmental sensors, communications, and lighting.

Cisco Security Operations Management Assessment

A primary component to FISMA is the ongoing security management capabilities and practices of the organization. Legacy security operations handled physical security and cybersecurity monitoring and incident response separately. Cisco's integrated, holistic approach to security operations management combines operations, using the IP infrastructure as a common platform to gain efficiency in reducing operational and capital costs.

Cisco Cloud Computing Security Assessment

As government agencies implement cloud computing architectures, new security policies and approaches must be implemented to protect the infrastructure. This assessment analyzes the controls that an agency has put into place around its cloud computing architecture. The assessment focuses on user access, security policy design, management, resiliency, and shared network interfaces.

Cisco Security Architecture Assessment Service Summary

By taking this comprehensive approach to assessing the security infrastructure, the Cisco Security Architecture Assessment Service helps your organization improve risk management and satisfy compliance needs by reducing threats to the confidentiality, integrity, and availability of business processes and information. (See Table 1.)

Table 1. Cisco Security Architecture Assessment Service Activity and Benefits Summary

Activity Summary	Benefit Summary
• Review security business goals, objectives, operations, and requirements • Review existing security architecture and design documentation, including physical and logical designs, operations processes, network topology diagrams, device configurations, and blueprints, as needed • For each functional domain included in the scope of the engagement, evaluate whether each of the recommended controls in the Cisco Security Control Framework is present in the security infrastructure and consistent with FISMA framework and NIST guidelines • Evaluate the effectiveness of each technical control at providing the designated security function by comparing the controls to ITILv3 and ISO 27000 standards • Evaluate the security architecture for scalability, performance, and manageability • Identify vulnerabilities in the security infrastructure (both cyber and physical) • Provide a report that documents control gaps, security risk analysis, and prioritized and actionable recommendations for remediation • Provide a presentation of findings and prioritized recommendations	• Create a robust and scalable security architecture using a business-focused, risk-avoidance approach • More effectively protect your infrastructure by identifying architectural vulnerabilities and deviations from security best practices and helping prioritize improvement areas • Safeguard employee productivity, primary intellectual property, and sensitive customer data by mitigating security risks • Address compliance requirements by improving internal controls to better protect data • Strengthen your security operational capabilities to prevent, detect, and respond to future threats • Protect your investment by extending the security capabilities of the existing infrastructure

Cisco Applied Expertise

Security architectural assessments are performed by Cisco security discipline consultants who draw upon their extensive security experience in government agencies and commercial industry to understand and recommend a more complete security solution. This expertise is supported by a combination of best-in-class tools, methodologies, and superior access to Cisco product development engineers to help you make the most of the sophisticated security features included in your Cisco products.

Cisco has experience designing and deploying world-class security operations centers. We conduct workflow and process mapping consistent with Six Sigma principles to design and improve customer security operations center environments. Cisco will also provide the systems integration to bring the best tools to operate and manage both cybersecurity and physical security.

Why Cisco Services

A primary component of the FISMA program is the ongoing management of security by the agency. Cisco brings its leadership and experience in security operations and management across the enterprise and service provider industries. Cisco has pioneered the industry in integrating security (cyber and physical) and safety operations management with its own converged security operations. We apply our expertise to assessing security operations work centers and tools.

Cisco Services make networks, applications, and the people who use them work better together. Today, the network and related infrastructure are a strategic platform in a world that demands better integration between people, information, and ideas. The IT infrastructure works better when services, together with products, create solutions aligned with business needs and opportunities. Cisco's unique approach to services defines the requisite activities at each phase of the IT lifecycle to help ensure service excellence. With a collaborative delivery methodology that joins the forces of Cisco, our skilled partners, and our customers, we achieve the best results.

To learn more about Cisco Security Services, visit **www.cisco.com/go/services/security** or contact your local account representative.

For more information on Cisco Federal Security solutions visit: **www.cisco.com/go/fedsecurity**

Availability and Ordering

Cisco Services are available globally from Cisco and our partners. Service delivery details may vary by region.

Cisco Services

Making Your Business
Work Smarter.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**